Employee Mobility Alert: Ends versus Means: Courts Vary in Their Interpretation of Employee Liability under the Computer Fraud and Abuse Act

10/15/2009

The federal courts are currently split on the question of whether an employee can be held civilly liable under the Computer Fraud and Abuse Act (CFAA) for misappropriating confidential company information that the employee is permitted to access within the scope of his or her employment. The CFAA, 18 U.S.C. § 1030 *et seq*., is primarily a criminal statute but provides for a private cause of action against a person who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains…information from any protected computer." 18 U.S.C. 1030(a)(2). Recently, the Ninth Circuit, in *LVRC Holdings LLC v. Brekka*, *et. al.*, joined a significant number of federal courts that have found that an employee who (before the termination of his or her employment) has permission to access the confidential information in question does not meet the definition of "without authorization" under the CFAA, regardless of the employee's improper motive or misuse of the information.

Brekka: Courts That Narrowly Apply the CFAA to Employer-Employee Disputes over Misuse of Company Information

In *Brekka*, the Ninth Circuit held that Christopher Brekka, a former employee of LVRC Holdings LLC (LVRC), did not violate the CFAA when he emailed proprietary company documents to his and his wife's personal email account during his employment with LVRC. According to the Court, LVRC was unable to demonstrate that Brekka "intentionally accessed a computer, without authorization or exceeding authorized access" under the CFAA, namely because LVRC gave Brekka permission to access the information at issue as a function of his employment with LVRC. Importantly, the Court held that because the CFAA did not define the term "authorization," the ordinary, common meaning of the term applied. The Court concluded that an "employer gives an employee 'authorization' to access a company computer when the employer gives the employee permission to use it." Thus, Brekka did not act without authorization or exceed authorized use because, as a function of his employment with LVRC, he had permission to access all of the confidential information at issue.

An increasing number of federal district courts share the Ninth Circuit's narrow interpretation of the CFAA, which limits the CFAA to an employee's unauthorized access, obtainment or alteration of information, and not the misuse or misappropriation of information obtained *with*

permission. A central rationale offered by these courts is that the text of the CFAA only prohibits improper "access" of computer information and does not explicitly prohibit misuse or misappropriation of information that is lawfully accessed. *See, e.g., Jet One Group, Inc. v. Halcyon Jet Holdings, Inc., et al.*, 2009 U.S. Dist. LEXIS 7259, at *18 (E.D.N.Y. Aug.14, 2009); *Condux Int'l Inc. v. Haugum*, 2008 U.S. Dist. LEXIS 100949, at *15 (D. Minn. Dec.15, 2008); *Int'l Ass'n of Mach. and Aerospace Workers v. Werner-Matsuda*, 390 F. Supp. 2d. 479, 499 (D. Md. 2005). These courts therefore focus on the scope of an employee's access to the confidential information rather than the employee's misuse of the information obtained. As in *Brekka*, these courts find that "without authorization" simply means "no access," and "exceeding authorized access" means to go beyond the permitted access granted to the employee. *See, e.g., Lockheed Martin Corp. v. Speed, et al.*, 2006 U.S. Dist. LEXIS 53108, at *19 (M.D. Fla. Aug. 1, 2006).

Additionally, courts in this line of cases focus on Congress' intent in enacting the CFAA, which was to prohibit "hacking" rather than an individual's misuse of data he or she has a lawful right to access. In support of this position, courts assert that the definition of "loss" or "damages" in the CFAA only make sense in the context of hacking. A civil cause of action cannot be maintained unless a person suffered "damage" or "loss," as defined in the statute. "Damages" are defined as "impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). "Loss" is defined as the "reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." § 1030(e)(1). Thus, this line of cases finds that to show "loss," employers must demonstrate more than revenue lost related to employee misappropriation of confidential information.

A final rationale asserted by the *Brekka* line of cases is that the CFAA is primarily a criminal statute and therefore, when confronted with two different interpretations, the court is obligated to apply the narrower one. *See, e.g., Condux* at *17; *Bridal Expo, Inc. et al. v. Van Floestein, et al.*, 2009 U.S. Dist. LEXIS 7388 (S.D. Tex. Feb. 3, 2009).

Citrin: Courts That Apply the CFAA More Broadly

On the opposite side of the spectrum are federal courts that interpret "without authorization" broadly, and find that an employee who permissibly accesses his or her employer's data for an improper purpose, such as misappropriation, violates the CFAA. In *International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), the Seventh Circuit held that an employee's misuse of an employer's confidential information constitutes a breach of the duty of loyalty that in effect ends the employee's authorized access to the employer's computer network. Similarly, in *Shugard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, the court found that once the employee acted on interests adverse to the employer and emailed trade secret information to the employer's competitor, he acted "without authorization" in violation of the CFAA. 119 F. Supp. 2d 1124 (W.D. Wash. 2000). This line of cases relies on a heavily criticized argument that once the employee's interests become adverse to the employer, the employee is no longer an agent of the employer and his permission to access the employer's confidential information ceases.

"Exceeding Access": The Role of Employee Handbooks, Employment Policies and Agreements

Employers with explicit employment policies and agreements limiting employee access to confidential company information may better be able to demonstrate that employees "exceeded" authorized use in violation of the CFAA. A few courts have found that employees "exceed authorization" when the terms of a contract that defines their authorized use of confidential information are violated. For example, the First Circuit, in *EF Cultural Travel BV v. Explorica, Inc.*, determined that a competitor and certain former employees exceeded the terms of a confidentiality agreement when they used a computer program to obtain large amounts of pricing data from the employer's websites. Additionally, in *United States v. Czubinksi,* the First Circuit found it relevant that the employee signed a policy limiting his computer-system use to "official purposes." In *Hewlett-Packard Company v. Byd:Sign, Inc.*, a Texas district court found that employees exceeded authorized use based on their executed confidentiality agreements and the employer's business conduct policies, which prohibited the employees from disclosing information and accessing or sending messages on HP's computer system for personal gain.

Important Points for Employers

As the law stands, employers in certain jurisdictions may or may not have viable claims under the CFAA against former employees for misuse or misappropriation of company information, depending on whether the courts in those jurisdictions apply *Citrin's* "ends" analysis or *Brekka's* "means" analysis. However, additional remedies may be available to employers for trade secret misappropriation or employee breaches of employment agreements. Employers should work with counsel to establish or review all agreements and employee policies that address employee computer and electronic systems usage. In particular, these agreements and policies should explicitly identify the scope of authorized activities and prevent employee access and distribution of confidential company information for unauthorized purposes.

* * *

Mintz Levin's **Employee Mobility Practice Group** is a multi–disciplinary, national group of practitioners with substantial experience in all aspects of the issues which arise relating to the movement of employees. Specifically, the group has successfully represented numerous companies and executives, in multiple industries, in litigating non-compete, trade secret and related issues in federal and state courts and arbitration forums throughout the U.S.; in negotiating arrangements that permit executives to transition to new positions while simultaneously protecting an employer's interests in preventing the disclosure of confidential information and trade secrets; in advising corporations on specific steps to protect corporate assets impacted by employee mobility; and in addressing employment lifecycle concerns that arise in the transactional context. Please contact any of the attorneys listed on this alert for more information.

For assistance in this area, please contact one of the attorneys listed below or any member of your Mintz Levin client service team.

MEMBERS

David Barmak
(202) 585-3507
DBarmak@mintz.com

Micha "Mitch" Danzig
(858) 314-1502
MDanzig@mintz.com

Jennifer B. Rubin
(212) 692-6766
JBRubin@mintz.com

Donald W. Schroeder
(617) 348-3077
DSchroeder@mintz.com

ASSOCIATES

Michael S. Arnold
(212) 692-6866
MArnold@mintz.com

Crystal Barnes
(202) 585-3594
CEBarnes@mintz.com

Katharine O. Beattie
(617) 348-1887
KOBeattie@mintz.com

Nathan R. Hamler
(858) 314-1510
NRHamler@mintz.com

Brandon T. Willenberg
(858) 314-1522
BTWillenberg@mintz.com